

Political Analysis on the Civil Cyber-Fraud Initiative

Madison Baughman

School of Cybersecurity, Old Dominion University

CYSE 525: Cybersecurity Strategy and Policy

Professor Duvall

February 22, 2026

The purpose of the Civil Cyber-Fraud Initiative is to crack down on fraud committed by government contractors lacking in federal compliance. This initiative uses the powers and protections of the False Claims Act to do so. In any government initiative or plan to address a problem in our nation, there are political implications and impacts to these strategies. A few political implications of the CCFI include the reinforcement of executive (Department of Justice) authority, the consideration of cybersecurity as a government spending issue, and the alignment with the goals of Executive Order 14028. Since its establishment the Department of Justice has been an enforcer of federal law and leader in ensuring public safety. Through the implementation of the CCFI, the purview and jurisdiction of the DOJ has been extended to the verification of cyber-framework compliance. Through this verification, the DOJ has an opportunity to assess whether or not companies are in violation of the False Claims Act by misrepresenting their compliance (Borgia & Bertch, 2021). Cybersecurity has long since been a concern when it comes to national data security, however new considerations highlight problems with government spending and fraudulent use of taxpayer money. When government contractors use taxpayer money under a falsely reported compliance status, they are essentially squandering limited government funds. Procurement spending between the years of 2000 and 2005 increased by 86%, taking up a large part of the federal budget (Lander, Kimball & Martyn, 2008). Now it is exponentially more, and fraud in this area can have drastic negative impacts on federal finances. Finally, Executive Order 14028, issued in May 2021 by President Biden was intended to improve national cybersecurity and modernize federal systems to meet growing cyber threats. Because of this order, companies are certifying under accredited certification bodies in the U.S. to meet cybersecurity standards (Bassett, 2021). This Executive Order is further enforced and upheld under the CCFI which seeks to enforce the utilization of cybersecurity standards.

Chuck Grassley is a Republican Senator from Iowa who has served in the Senate since 1981. Before his time in the Senate he also served in the U.S. House of Representatives for 6 years and the Iowa House of Representatives for 16 years. Senator Grassley was a key figure in amending the False Claims Act in 2023 to strengthen the FCA and close loopholes that threaten the security of federal funding. Senator Grassley along with Representative Berman who also worked on the updates to the FCA claimed that their proposed amendments would give special permission to government employees in situations involving whistleblowing while delegating the power to dismiss these actions under certain circumstances to the government (Estrada, 2008). Grassley's motivation and concern behind these amendments was the potential for loss of federal funding to fraud, a concern well addressed in the Civil Cyber-Fraud Initiative. Although before the time of the CCFI, these amendments address specific concerns within the initiative and pave the way for its successful implementation. The protections given to government employees allow the flagging of falsely reporting cyber-framework compliance, and the reservation of government power to dismiss or intervene in cases supports the alignment of the CCFI with national security priorities. These concerns and later amendments by Senator Grassley limited ambiguity in the FCA and clarified protections that would later support and empower the Civil Cyber-Fraud Initiative.

Patrick Leahy represented the state of Vermont for 48 years in the U.S. Senate. Senator Leahy retired in January 2023 after serving eight consecutive terms. In a 2009 committee report, Leahy referred to the FCA as "an extraordinary civil enforcement tool used to recover funds lost to fraud and abuse.". Leahy also goes on to remark on improvements to the FCA, aimed at deterring fraud and recovering taxpayer dollars (Love, 2012). From these statements we can see that Leahy was very concerned with the scope of federal funds lost to fraud. His opinion that

fraud must be deterred and restitution made comes from a demand for justice for taxpayers and those that have been essentially stolen from. These statements by Senator Leahy apply directly to the Civil Cyber-Fraud Initiative in the way the CCFI addresses Leahy's call to action. The CCFI outlines expectations for contractors to avoid fraudulent activity and institutes a punishment for when it is discovered that they did not. In this way fraudulent activity is addressed and offenders of the FCA are held accountable. These decisions by Senator Leahy express a need for more legislation and action against fraud, and the implementation of the CCFI effectively addresses those needs.

Edward Kaufman served in the U.S. Senate from January 2009 to November 2010 for the state of Delaware to fill the vacancy of then appointed Vice President Joe Biden. In the context of a debate on medical care kickbacks, the FCA was invoked to assess whistleblower incentives. According to Senator Kaufman, whistleblower actions were strengthened under new legislature and that prior court decisions defeated enforcement efforts (McGirty, 2024). In these statements, Kaufman emphasises the importance of incentivizing whistleblowers and not preventing pursuance of these claims. He makes this statement because in an age of prolific fraud, whistleblowers are the first line of defense in recognizing and acting against it. If whistleblowers aren't protected and/or incentivized, that resource is likely to be lost. The CCFI addresses these concerns from Kaufman by implementing the FCA protections for whistleblowers and ensuring that actions taken against fraudulent government contractor activity reward them. Kaufman's concerns are extremely relevant today to ensuring whistleblowers are protected. The ramifications of Kaufman's decisions on the needs of whistleblowers are an assurance that their needs are kept in mind and that the resource is not under-appreciated.

Citations

Bassett, R. (2021). ISAGCA Responds to NIST Call for Standards to Fulfill Executive Order 14028. *Intech*, 68(4), 42-43.

<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/isagca-responses-nist-call-standards-fulfill/docview/2559714152/se-2>

Borgia, M. T., & Bertch, K. (2021). Warning of "Very Hefty Fines," DOJ Launches Civil Cyber-Fraud Initiative to Pursue Violations of Cybersecurity Requirements in Government Contracts. *Journal of Health Care Compliance*, 23(5), 25-26,40.

<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/warning-very-hefty-fines-doj-launches-civil-cyber/docview/2630357175/se-2>

Estrada, L. A. (2008). Congress to Consider Dramatic Expansion of False Claims Act. *Journal of Health Care Compliance*, 10(2), 5-10.

<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/congress-consider-dramatic-expansion-false-claims/docview/227930824/se-2>

Lander, G. H., Kimball, V. J., & Martyn, K. A. (2008). Government Procurement Fraud: Certified Public Accountant. *The CPA Journal*, 78(2), 16-22,24.

<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/government-procurement-fraud/docview/212237827/se-2>

Love, Cynthia. (2012). The fraud enforcement and recovery act of 2009 and the expansion of liability under the false claims act. *Utah Law Review*, 2012(2), 1129-1154.

<https://heinonline.org/HOL/P?h=hein.journals/utahlr2012&i=1145>

McGirty, Andrew. (2024). Cracking causation: the need for a workable link between the anti-kickback statute and false claims act. *Case Western Reserve Law Review*, 75(1), 429-[x]. <https://heinonline.org/HOL/P?h=hein.journals/cwrlrv75&i=437>